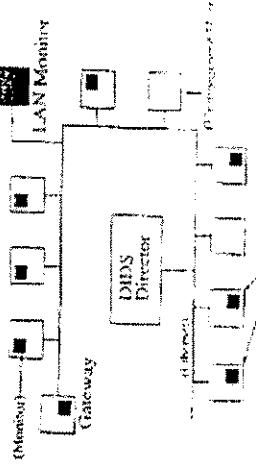


Internetwork Security Monitor “ISM”

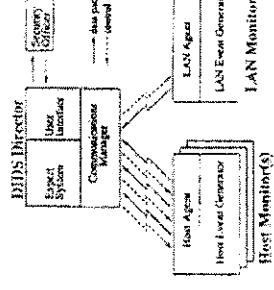
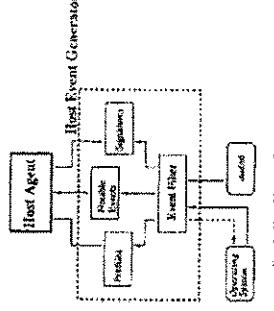
| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|--|--|--|
| 1 | A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising: | <p>“To address these limitations, we designed a model, called the Internetwork Security Monitor (ISM), to perform intrusion detection in a highly interconnected wide-area network.” (263) [SYM_P_0069245]</p> <p>“In extending the LAN monitoring capabilities into an internetwork environment, we are exploring the feasibility of different design alternatives for distributed-network traffic monitoring and analysis...” (263) [SYM_P_0069245]</p> <p>“We are designing and implementing a prototype Distributed Intrusion Detection System (DIDS) that combines distributed monitoring and data reduction (through individual host and LAN monitors) with centralized data analysis (through the DIDS director) to monitor a heterogeneous network of computers. This approach is unique among current IDS’s.” (167) [SYM_P_0077175]</p> | |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|-------------------------------------|---|
| | |  <p>The diagram illustrates a network security architecture. At the top left is a box labeled "Gateway". To its right is a box labeled "LAN Monitoring". Below the "Gateway" is a box labeled "DNS Director". A horizontal line labeled "bus" connects the "Gateway", "LAN Monitoring", and "DNS Director". On the right side of the "bus" line is a box labeled "User". A dashed line labeled "DIDS Target Environment" extends from the "User" box downwards.</p> <p style="text-align: center;">Fig. 4. DIDS Target Environment</p> <p style="text-align: right;">(176) [SYM P 0077184]</p> |

330289_1

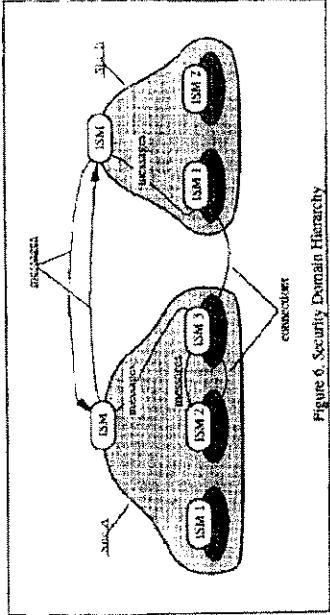
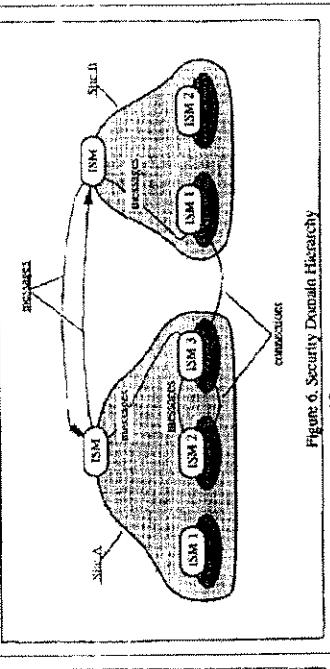
**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | |
|-------------------------|------------|---|---|
| | |  <p>ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)</p> <p>BIDS Director Security Officer Expert System User Interface Compliance Manager</p> <p>LAN Agent LAN Event Generator</p> <p>LAN Monitor</p> <p>Host Agent Host Level Monitoring</p> <p>Host Monitor(s)</p> <p>Fig. 1. Communications Architecture</p> |  <p>Host Agent</p> <p>Root Event Generator</p> <p>Rule Engine</p> <p>Rule Filter</p> <p>Operating System</p> <p>Fig. 2. Host Monitor System</p> |

(176) [SYM P 007718]
“An individual site (e.g., a university or government research
deploying a plurality of

330289_1

Internetwork Security Monitor “ISM”

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) <p>facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines.” (270) [SYM_P_0069252]</p> | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) <p>facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines.” (270) [SYM_P_0069252]</p> |
|-------------------------|------------|--|---|
| | |  <p>Figure 6. Security Domain Hierarchy</p> <p>(270) [SYM_P_0069252]</p> |  <p>Figure 6. Security Domain Hierarchy</p> <p>(270) [SYM_P_0069252]</p> <p>This paper describes a prototype Distributed Intrusion Detection System (DIDS) which generalizes the target environment in order to monitor multiple hosts connected via a network as well as the network itself. The DIDS components include the DIDS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network. The information gathered by these distributed components is transported to, and</p> |

330289_1

**Internet Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|------------|---------------------------------------|--|
| | | | |

analyzed at, a central location (viz. an expert system, which is a sub-component of the director), thus providing the capability to aggregate information from different sources. We can cope with any audit trail format as long as the events of interest are provided.” (168) [SYM_P_0077176]

“The objective of the model is to significantly improve our capability to detect and react to intrusions into an arbitrary wide-area network (WAN) (e.g., the Internet) through a distributed intrusion-detection and analysis system. The system will monitor the various component networks of the internetwork and bring potentially intrusive behavior to the attention of the local-network security managers.” (262) [SYM_P_0069244]

“The NSM, initially designed to detect intrusive activity across a local-area network (LAN), already augments DIDS’ analysis capability by scrutinizing network activity into hosts which do not support host monitors; therefore, all hosts in the DIDS domain can be monitored to a certain level for the presence of intrusive activity.” (265) [SYM_P_0069244]

“We now present an architecture based on NSM and DIDS which provides for intrusion detection and accountability in large-scale interconnected networks (e.g., the Internet).” (268) [SYM_P_0069250]

The objective of the model is to significantly improve our capability to detect and react to intrusions into an arbitrary wide-area network (WAN) (e.g., the Internet) through a distributed intrusion-detection and analysis system. The system will monitor the various component networks of the internetwork and bring potentially intrusive behavior to the attention of the local-network security managers.” (262) [SYM_P_0069244]

“The NSM, initially designed to detect intrusive activity across a local-area network (LAN), already augments DIDS’ analysis capability by scrutinizing network activity into hosts which do not support host monitors; therefore, all hosts in the DIDS domain can be monitored to a certain level for the presence of intrusive activity.” (265) [SYM_P_0069247]

“We now present an architecture based on NSM and DIDS which provides for intrusion detection and accountability in large-scale interconnected networks (e.g., the Internet).” (268) [SYM_P_0069250]

**Internetes Security Monitor
“ISM”**

| 203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|---------------------------------|-------------------|---|--|
| | | <p>“The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called <i>doorknob</i> attack. In a doorknob attack the intruder’s goal is to discover, and gain access to, insufficiently-protected hosts on a system. The intruder generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis’ NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a password for the super-user account. In this case, the intruder used <i>telnet</i> to make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an attack on the individual host, current IDS’s are generally unable to correlate reports from multiple hosts; thus they cannot recognize the <i>doorknob</i> attack as such. Because DIDS aggregates and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even though there may be too few on a single host to alert that host’s monitor.</p> | <p>In another incident, our NSM recently observed an intruder</p> |

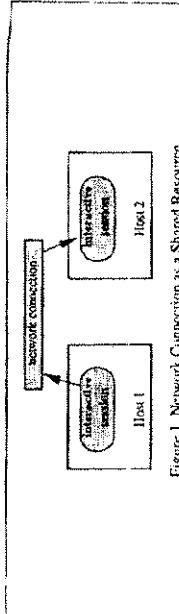
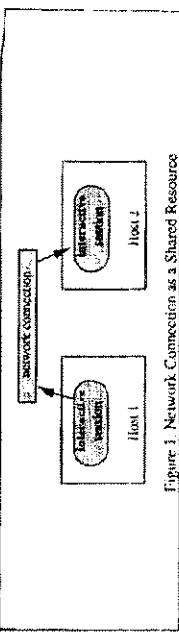
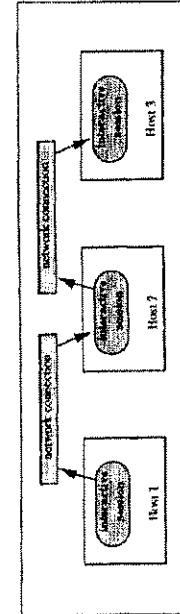
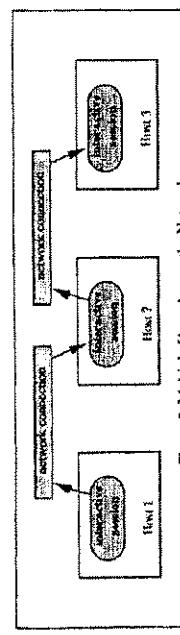
**Internetes Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|------------|---------------------------------------|---|
| | | | <p>gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack.</p> <p>Another possible scenario is what we call <i>network browsing</i>. This occurs when a (network) user is looking through a number of files on several different computers within a short period of time. The browsing activity level on any single host may not be sufficiently high enough to raise any alarm by itself. However, the network-wide, aggregated browsing activity level may be high enough to raise suspicion on this user. Network browsing can be detected as follows. Each host monitor will report that a particular user is browsing on that system, even if the corresponding degree of browsing is small. The expert system can then aggregate such information from multiple hosts to determine that all of the browsing activity corresponds to the same network user. This</p> |

**Internetwor Security Monitor
“ISM”**

| '203 Claim number | Claim Term ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|---|
| | | <p>scenario presents a key challenge for DIDS: the tradeoff between sending all audit records to the director versus missing attacks because thresholds on each host are not exceeded.</p> <p>In addition to the specific scenarios outlined above, there are a number of general ways that an intruder can use the connectivity of the network to hide his trail and to enhance his effectiveness. Some of the attack configurations which have been hypothesized include <i>chain</i> and <i>parallel</i> attacks [2]. DIDS combats these inherent vulnerabilities of the network by using the very same connectivity to help track and detect the intruder. Note that DIDS should be at least as effective as host-based IDS's (if we implement all of their functionality in the DIDS host monitor), and at least as effective as the stand-alone NSM.' (168-69)</p> <p>[SYM_P_0077176-SYM_P_0077177]</p> |
| | | <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks.” (264) [SYM_P_0069246]</p> <p>“The tracking between users and hosts is performed by treating a network connection as a shared resource and determining which users are accessing that resource. For example, if a user creates a remote login session (called session2), on host2, DIDS first identifies the host-to-host connection (called net-rsrc) responsible for the session and binds the information as the pair <net-rsrc,</p> |

Internetwork Security Monitor “ISM”

| | | | |
|------------------------------------|--|---|---|
| ‘203 Claim number | Claim Term <pre>packet};</pre> | <p>ISM – 102(b) (printed publication)</p> <p>session2@host2>. DIDS then determines which session on host1 meets the requirements <net-rsrc, ?@host1>, and tracking is achieved (see Figure 1).” (265) [SYM_P_0069247]</p>  <p>Figure 1. Network Connection as a Shared Resource</p> | <p>ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)</p> <p>session2@host2>. DIDS then determines which session on host1 meets the requirements <net-rsrc, ?@host1>, and tracking is achieved (see Figure 1).” (265) [SYM_P_0069247]</p>  <p>Figure 1. Network Connection as a Shared Resource</p> |
| | | | <p>“The NSM, initially designed to detect intrusive activity across a local-area network (LAN), already augments DIDS’ analysis capability by scrutinizing network activity into hosts which do not support host monitors...” (265) [SYM_P_0069247]</p>  <p>Figure 2. Multiple Hops Across the Network</p> |
| | | | <p>(266) [SYM_P_0069248]</p>  <p>Figure 2. Multiple Hops Across the Network</p> |

**Internet Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|---|
| | | <p>“Like the host monitor, the LAN monitor consists of a <i>LAN event generator</i> (LEG) and a <i>LAN agent</i>. The LEG is currently a subset of UC Davis’ NSM [3]. Its main responsibility is to observe all of the traffic on its segment of the LAN to monitor host-to-host connections, services used, and volume of traffic. The LAN monitor reports on such network activity as <i>rlogin</i> and <i>telnet</i> connections, the use of security-related services, and changes in network traffic patterns.” (169) [SYM_P_0077177]</p> <p>“An event reported by a LAN monitor is called a network audit record (nar). The record syntax is: <i>nar(Monitor-ID, Source_Host, Dest_Host, Time, Service, Domain, Status)</i>.” (172) [SYM_P_0077180]</p> <p>“The LAN monitor is currently a subset of UC Davis’ Network Security Monitor [3]. The LAN monitor builds its own ‘LAN audit trail’. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection.” (171) [SYM_P_0077179]</p> |
| | generating, by the monitors, reports of said suspicious | <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks.”</p> |

330289_1

49

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|-----------------------|--|--|
| activity; and | (264) [SYM_P_0069246] | <p>In extending the LAN monitoring capabilities into an internetwork environment, we are exploring the feasibility of different design alternatives for distributed-network traffic monitoring and analysis, including the following hierarchical architecture. Under this architecture, independent monitors are placed at various locations over an internetworked environment. These monitors exchange and share information (including those on hypothesized attacks) to detect possible security breaches. Subnetworks, in turn, exchange information among one another to detect inter-subnetwork attacks. (263)</p> <p>“An event reported by a LAN monitor is called a network audit record (nar). The record syntax is: nar(Monitor-ID, Source_Host, Dest_Host, Time, Service, Domain, Status).” (172) [SYM_P_0077180]</p> <p>“An event reported by a host monitor is called a host audit record (har). The record syntax is: har(Monitor-ID, Host-ID, Audit-UID, Real-UID, Effective-UID, Time, Domain, Action, Transaction, Object, Parent Process, PID, Return Value, Error Code).” (171) [SYM_P_0077179]</p> | |
| | | | <p>“Multiple DIDS-like monitors, called ISM domain monitors, communicating through well-defined protocols form the core of</p> |

Internet Network Security Monitor “ISM”

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|--|------------|--|---|
| suspicious activity, by one or more hierarchical monitors. | | <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks.” (264) [SYM_P_0069246]</p> <p>“When a user initiates a connection from a host in one ISM domain to a host in a second ISM domain, the ISMs may exchange information to allow a more accurate analysis of the security state of their own domains.” (268) [SYM_P_0069250]</p> <p>“Access to this analysis by external ISMs are made by the following requests:</p> <p>“GET ANALYSIS HOST-ID <host-address></p> <p>“GET ANALYSIS HOST-T-ID <host-address></p> <p>The second request also returns a value between 0 and 100, indicating whether or not the ISM believes that the host is associated with intrusive activity. The host does not necessarily have to be within the ISM’s domain. For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile user on it.” (268-269) [SYM_P_0069250- SYM_P_0069251]</p> | <p>the distributed ISM.” (264) [SYM_P_0069246]</p> <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks.” (264) [SYM_P_0069246]</p> <p>“When a user initiates a connection from a host in one ISM domain to a host in a second ISM domain, the ISMs may exchange information to allow a more accurate analysis of the security state of their own domains.” (268) [SYM_P_0069250]</p> <p>“Access to this analysis by external ISMs are made by the following requests:</p> <p>“GET ANALYSIS HOST-ID <host-address></p> <p>“GET ANALYSIS HOST-T-ID <host-address></p> <p>The second request also returns a value between 0 and 100, indicating whether or not the ISM believes that the host is associated with intrusive activity. The host does not necessarily have to be within the ISM’s domain. For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile user on it.” (268-269) [SYM_P_0069250- SYM_P_0069251]</p> |

330289_1

“The ISM model also allows ISMs to be grouped hierarchically.

**Internetwork Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|----------------------------------|-------------------|--|--|
| | | <p>For example, ISM1’ may monitor a domain which is divided into three sub-domains, each with its own ISM sub-monitors. This hierarchical structure provides two major benefits. First, because the ISM1’ domain can look into its sub-domains, it can aggregate a user’s activities across these sub-domains.” (269) [SYM_P_0069251]</p> <p>“We are designing and implementing a prototype Distributed Intrusion Detection System (DIDS) that combines distributed monitoring and data reduction (through individual host and LAN monitors) with centralized data analysis (through the DIDS director) to monitor a heterogeneous network of computers. This approach is unique among current IDS’s.” (167) [SYM_P_0077175]</p> <p>“The information gathered by these distributed components is transported to, and analyzed at, a central location (<i>viz.</i> an expert system, which is a sub-component of the director), thus providing the capability to aggregate information from different sources. We can cope with any audit trail format as long as the events of interest are provided.” (168) [SYM_P_0077176]</p> <p>“The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called <i>doorknob</i> attack. In a doorknob attack the intruder’s goal is to discover, and gain access</p> | |

**Internetwork Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term (printed publication) | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|----------------------------------|---|--|--|
| | | <p>to, insufficiently-protected hosts on a system. The intruder generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis’ NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a password for the super-user account. In this case, the intruder used <i>telnet</i> to make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an attack on the individual host, current IDS’s are generally unable to correlate reports from multiple hosts; thus they cannot recognize the <i>doorknob</i> attack as such. Because DIDS aggregates and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even though there may be too few on a single host to alert that host’s monitor.</p> <p>In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS’s (e.g., changing passwords and failed events). In an incident such</p> | |

**Internetes Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) |
|--|---|---------------------------------------|
| ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) | | |
| | <p>as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack.</p> <p>Another possible scenario is what we call <i>network browsing</i>. This occurs when a (network) user is looking through a number of files on several different computers within a short period of time. The browsing activity level on any single host may not be sufficiently high enough to raise any alarm by itself. However, the network-wide, aggregated browsing activity level may be high enough to raise suspicion on this user. Network browsing can be detected as follows. Each host monitor will report that a particular user is browsing on that system, even if the corresponding degree of browsing is small. The expert system can then aggregate such information from multiple hosts to determine that all of the browsing activity corresponds to the same network user. This scenario presents a key challenge for DIDS: the tradeoff between sending all audit records to the director versus missing attacks because thresholds on each host are not exceeded.</p> | |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) |
|-------------------------|------------|--|
| | | <p>ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)</p> <p>In addition to the specific scenarios outlined above, there are a number of general ways that an intruder can use the connectivity of the network to hide his trail and to enhance his effectiveness. Some of the attack configurations which have been hypothesized include <i>chain</i> and <i>parallel</i> attacks [2]. DIDS combats these inherent vulnerabilities of the network by using the very same connectivity to help track and detect the intruder. Note that DIDS should be at least as effective as host-based IDS’s (if we implement all of their functionality in the DIDS host monitor), and at least as effective as the stand-alone NISM.” (168-69) [SYM_P_0077176- SYM_P_0077177]</p> <p>“The DIDS architecture combines distributed monitoring and data reduction with centralized data analysis.” (169) [SYM_P_0077177]</p> <p>“Reports are sent independently and asynchronously from the host and LAN monitors to the DIDS director through a communications infrastructure (Fig. 2). High level communication protocols between the components are based on the ISO Common Management Information Protocol (CMIP) recommendations, allowing for future inclusion of CMIP management tools as they become useful. The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly</p> |

**Internetwork Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|------------|---------------------------------------|---|
| | | | <p>reports from the monitors. The director can also make requests for more detailed information from the distributed monitors via a ‘GET’ directive, and issue commands to have the distributed monitors modify their monitoring capabilities via a ‘SET’ directive.” (169) [SYM_P_0077177]</p> <p>“The expert system is responsible for evaluating and reporting on the security state of the monitored system. It receives the reports from the host and the LAN monitors, and, based on these reports, it makes inferences about the security of each individual host, as well as the system as a whole.” (169) [SYM_P_0077177]</p> <p>“Correlating data from several independent sources, including the network itself, can aid in recognizing this type of behavior and tracking an intruder to their source.” (170) [SYM_P_0077178]</p> <p>“The expert system uses rules derived from the hierarchical Intrusion Detection Model (IDM). The IDM describes the data abstractions used in inferring an attack on a network of computers. That is, it describes the transformation from the distributed raw audit data to high level hypotheses about intrusions and about the overall security of the monitored environment. In abstracting and correlating data from the distributed sources, the model builds a virtual machine which consists of all the connected hosts as well as the network itself. This unified view of the distributed system simplifies the</p> |

**Internetes Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|------------|--|--|
| | | <p>recognition of intrusive behavior which spans individual hosts. The model is also applicable to the trivial network of a single computer.” (172) [SYM_P_0077180]</p> <p>“Events in context are combined to create threats.” (172) [SYM_P_0077180]</p> | <p>“At the highest level, the model produces a numeric value between one and 100 which represents the overall <i>security state</i> of the network. The higher the number the less secure the network. This value is a function of all the threats for all the subjects on the system. Here again we treat the collection of hosts as a single distributed system. Although representing the security level of the system as a single value seems to imply some loss of information, it provides a quick reference point for the SSO. In fact, in the current implementation, no information is lost since the expert system maintains all the evidence used in calculating the security state in its internal database, and the SSO has access to that database.” (173) [SYM_P_0077181]</p> <p>“The expert system shell consists of approximately a hundred lines of Prolog source code. The shell is responsible for reading new facts reported by the distributed monitors, attempting to apply the rules to the facts and hypotheses in the Prolog database, reporting suspected intrusions, and maintaining the various dynamic values associated with the rules and hypotheses.” (173) [SYM_P_0077181]</p> |

330289_1

**Internetes Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|--|--|
| | | <p>“In addition to the consideration of external temporal context, the expert system uses time windows to correlate events occurring in temporal proximity. This notion of temporal proximity implements the heuristic that a call to the UNIX <i>who</i> command followed closely by a <i>login</i> or <i>logout</i> is more likely to be related to an intrusion than either of those events occurring alone. Spatial context implies the relative importance of the source of events. That is, events related to a particular user, or events from a particular host, may be more likely to represent an intrusion than similar events from a different source. For instance, a user moving from a low-security machine to a high-security machine may be of greater concern than a user moving in the opposite direction. The model also allows for the correlation of multiple events from the same user or source. In both of these cases, the multiple events are more noteworthy when they have a common element than when they do not.” (172) [SYM_P_0077180]</p> | <p>See '203 claim 1</p> <p>“For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile user on it.” (269) [SYM_P_0069251]</p> |
| 2 | The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities. | | <p>See '203 claim 1</p> <p>“For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile user on it.” (269) [SYM_P_0069251]</p> |

Internetwork Security Monitor
“ISM”

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|------------|---|--|
| | | <p>“Other functionality for an ISM, while helpful but not required, includes the ability to analyze the activity within the domain for intrusive activity. Access to this analysis by external ISMs are made by the following requests:</p> <pre> GET ANALYSIS CONN-ID <id> GET ANALYSIS HOST-ID <host-address> GET ANALYSIS SERVICE <service-name> GET ANALYSIS VULNERABILITY <vulnerability-id></pre> | <p>“Other functionality for an ISM, while helpful but not required, includes the ability to analyze the activity within the domain for intrusive activity. Access to this analysis by external ISMs are made by the following requests:</p> <pre> GET ANALYSIS CONN-ID <id> GET ANALYSIS HOST-ID <host-address> GET ANALYSIS SERVICE <service-name> GET ANALYSIS VULNERABILITY <vulnerability-id></pre> <p>The first request returns a value between 0 and 100, which indicates whether or not the ISM believes that the user owning the connection given by <id> is behaving intrusively. The second request also returns a value between 0 and 100, indicating whether or not the ISM believes that the host is associated with intrusive activity. The host does not necessarily have to be within the ISM’s domain. For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile user on it. The third request returns a value between 0 and 100 indicating the ISM’s belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet worm exploited a hole in the mail service). The last request returns a value between 0 and 100 indicating the ISM’s belief that a particular vulnerability has recently been exploited. To perform this, the ISM must have a</p> |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|--|---|--|
| | | <p>catalog of known vulnerabilities and signatures to detect their [attempted] exploitation. Due to the sensitive nature of vulnerabilities, some ISMs (e.g., those at government sites) may have a more complete listing than other ISMs (e.g., those at universities).” (268-269) [SYM_P_0069250- SYM_P_0069251]</p> <p>In extending the LAN monitoring capabilities into an internetwork environment, we are exploring the feasibility of different design alternatives for distributed-network traffic monitoring and analysis, including the following hierarchical architecture. Under this architecture, independent monitors are placed at various locations over an internetworked environment. These monitors exchange and share information (including those on hypothesized attacks) to detect possible security breaches. Subnetworks, in turn, exchange information among one another to detect inter-subnetwork attacks. (263) [SYM_P_0069245]</p> | <p>catalog of known vulnerabilities and signatures to detect their [attempted] exploitation. Due to the sensitive nature of vulnerabilities, some ISMs (e.g., those at government sites) may have a more complete listing than other ISMs (e.g., those at universities).” (268-269) [SYM_P_0069250- SYM_P_0069251]</p> <p>In extending the LAN monitoring capabilities into an internetwork environment, we are exploring the feasibility of different design alternatives for distributed-network traffic monitoring and analysis, including the following hierarchical architecture. Under this architecture, independent monitors are placed at various locations over an internetworked environment. These monitors exchange and share information (including those on hypothesized attacks) to detect possible security breaches. Subnetworks, in turn, exchange information among one another to detect inter-subnetwork attacks. (263) [SYM_P_0069245]</p> <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Snag1]) into arbitrarily wide networks.” (264) [SYM_P_0069246]</p> <p>“We anticipate that a growing set of tools, including incident-handling tools and network-management tools, will be used in conjunction with the intrusion-detection functions of DIDS. This will give the SSO the ability to actively respond to attacks against the system in real-time. Incident-handling tools may consist of</p> |
| 3 | The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack. | “Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Snag1]) into arbitrarily wide networks.” (264) [SYM_P_0069246] | |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|--|--|
| | | <p>possible courses of action to take against an attacker, such as cutting off network access, a directed investigation of a particular user, removal of system access, etc. Network-management tools that are able to perform network mapping would also be useful.” (169-70) [SYM_P_0077177- SYM_P_0077178]</p> <p>“The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly reports from the monitors.” (169) [SYM_P_0077177]</p> <p>“The ISM model links together security systems monitoring particular domains (e.g., a DIDS-monitored domain) via standard information exchange protocols such as the Common Management Information Protocol (CMIP) to create a large-scale, highly distributed intrusion-detection system.” (268) [SYM_P_0069250]</p> <p>“Finally, security workbenches allow network managers to logon to their local ISM domain monitor to examine the results of the monitor’s analysis, query further into possible intrusions, exchange information with other network security managers, and administer various security tools such as Security Profile Inspector (SPI) or Computer Oracle Password Security system (COPS).” (264) [SYM_P_0069246]</p> | |
| 4 | <p>The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.</p> | | |

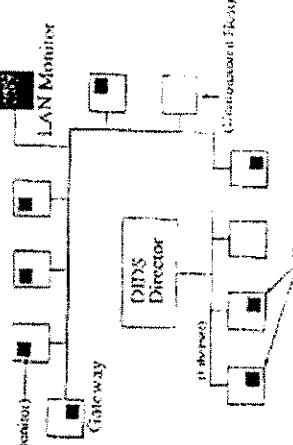
**Internetes Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|----------------------------------|---|--|--|
| | | | <p>“High level communication protocols between the components are based on the ISO Common Management Information Protocol (CMIP) recommendations, allowing for future inclusion of CMIP management tools as they become useful.” (169) [SYM_P_0077177]</p> |
| 5 | The method of claim 1, wherein the enterprise network is a TCP/IP network. | <p>“GET CONNECTION TCP/IP-DEF <def> TIME <time></p> <p>... The second request (with the time given in the remote ISM’s time frame) returns an identifier, which can be used to make further requests.” (268) [SYM_P_0069250]</p> | <p>“GET CONNECTION TCP/IP-DEF <def> TIME <time></p> <p>... The second request (with the time given in the remote ISM’s time frame) returns an identifier, which can be used to make further requests.” (268) [SYM_P_0069250]</p> |

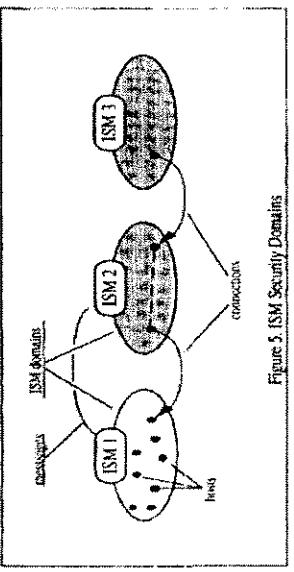
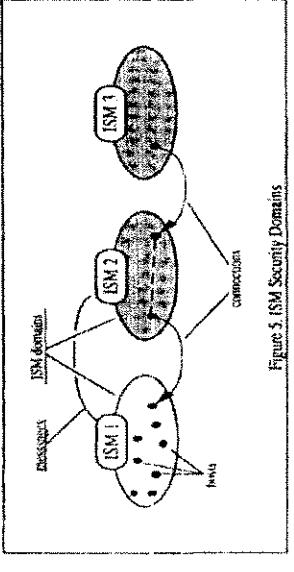
**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|--|---|--|
| | | Internet.” (270-271) [SYM_P_0069252- SYM_P_0069253] | <p>The LAN monitor is currently a subset of UC Davis’ Network Security Monitor [3]. The LAN monitor builds its own “LAN audit trail”. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. (171) [SYM_P_0077179]</p> <p>“An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines.” (270) [SYM_P_0069252]</p> <p>“In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment.” (174) [SYM_P_0077182]</p> |
| 6 | The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}. | “An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines.” (270) [SYM_P_0069252] | |

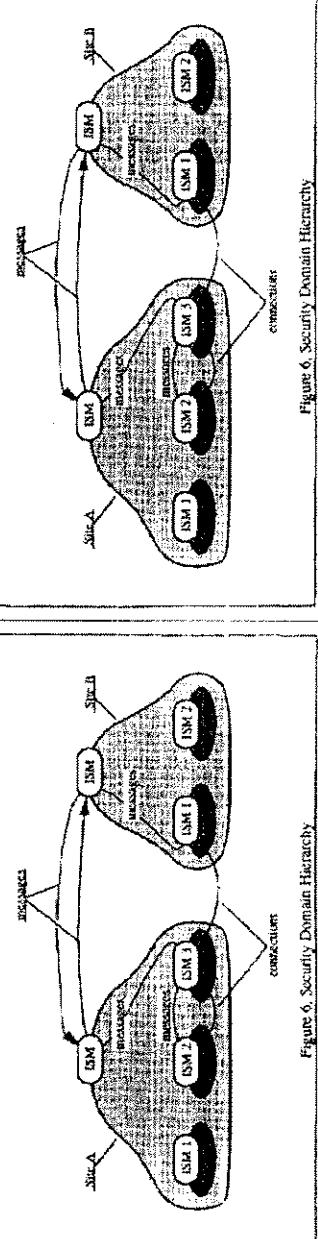
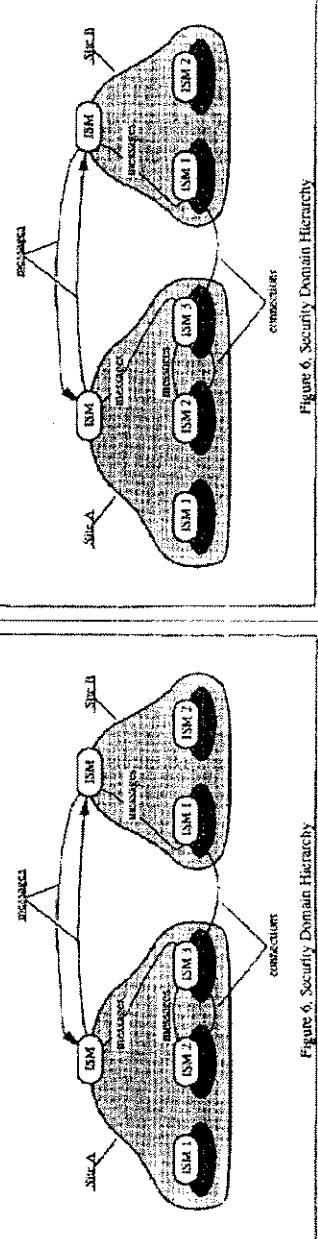
**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|------------|--|--|
| | |  <p>The diagram illustrates a DBMS Target Environment. At the top level is a 'LAN Monitor'. Below it is a 'Gateway'. A 'Monitor' is connected to both the 'Gateway' and a 'DNS Director'. The 'DNS Director' is connected to three 'Subnets'. Each 'Subnet' contains a 'Router' and a 'Block'. The 'Router' is connected to a 'Client'.</p> | <p>Fig. 1. DBMS Target Environment</p> <p>[SYM_P_0077184]</p> <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna9]) into arbitrarily wide networks.” (264) [SYM_P_0069246]</p> <p>“The ISM model also allows ISMs to be grouped hierarchically. For example, ‘ISM1’ may monitor a domain which is divided into three sub-domains, each with its own ISM sub-monitors. This hierarchical structure provides two major benefits. First, because the ‘ISM1’ domain can look into its sub-domains, it can aggregate</p> <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna9]) into arbitrarily wide networks.” (264) [SYM_P_0069246]</p> <p>“The ISM model also allows ISMs to be grouped hierarchically. For example, ‘ISM1’ may monitor a domain which is divided into three sub-domains, each with its own ISM sub-monitors. This hierarchical structure provides two major benefits. First, because the ‘ISM1’ domain can look into its sub-domains, it can aggregate</p> |
| 7 | | | <p>The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.</p> |

**Internetwork Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|--|---|
| | <p>a user's activities across these sub-domains.” (269) [SYM_P_0069251]</p>  <p>Figure 5 [ISM Security Domains] (269) [SYM_P_0069251]</p> | <p>a user's activities across these sub-domains.” (269) [SYM_P_0069251]</p>  <p>Figure 5 [ISM Security Domains] (269) [SYM_P_0069251]</p> |

**Internetwork Security Monitor
“ISM”**

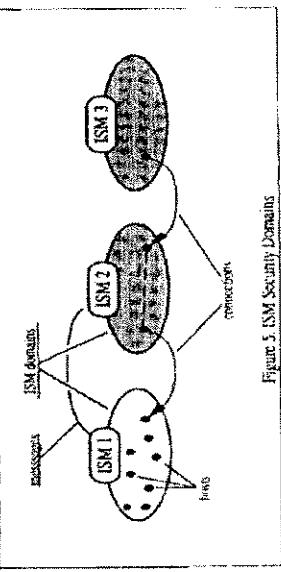
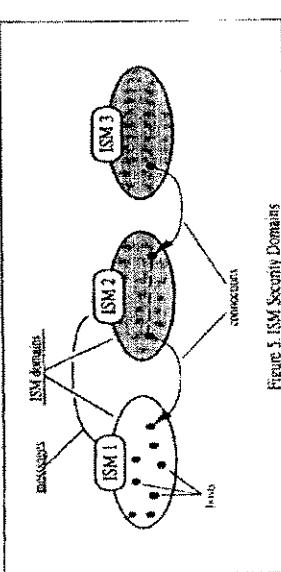
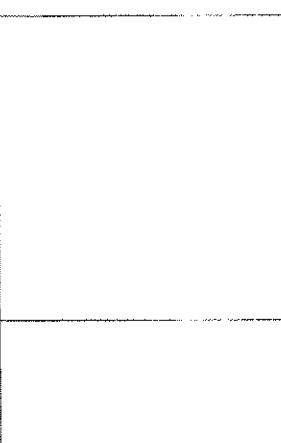
| '203 Claim number | Claim Term | ISM – 102(b) (printed publication)  ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)  |
|-------------------------|------------|---|
| | | <p>(270) [SYM_P_0069252]</p> <p>“In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment.” (174) [SYM_P_0077182]</p> <p>“The DIDS components include the DIDS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network.” (168) [SYM_P_0077176]</p> <p>“In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS’s</p> |

330289_1

**Internet Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|--|---|--|
| | | | <p>(e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most DIDS’s would report the occurrence of an incident involving user “guest” on the target machine, DIDS would also report that user “guest” was really, for example, user “smith” on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the “chain” to find the initial launching point of the attack.” (168) [SYM_P_0077176]</p> |
| 8 | The method of claim 7, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor’s associated network domain. | <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks.” (264) [SYM_P_0069246]</p> | <p>“Primarily, the ISM extends the Distributed Intrusion Detection System (DIDS) (see [Sna91]) into arbitrarily wide networks.” (264) [SYM_P_0069246]</p> <p>“The ISM model also allows ISMs to be grouped hierarchically. For example, ‘ISM1’ may monitor a domain which is divided into three sub-domains, each with its own ISM sub-monitors. This hierarchical structure provides two major benefits. First, because the ‘ISM1’ domain can look into its sub-domains, it can aggregate a user’s activities across these sub-domains.” (269) [SYM_P_0069251]</p> |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) |
|-------------------------|------------|--|
| | | <p>ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)</p>  <p>Figure 5. ISM Security Domains</p> <p>(269) [SYM_P_0069251]</p> |
| | |  <p>Figure 5. ISM Security Domains</p> <p>(269) [SYM_P_0069251]</p> |
| | |  <p>Figure 5. ISM Security Domains</p> <p>(269) [SYM_P_0069251]</p> |

330289_1

**Internet Security Monitor
“ISM”**

| Claim number | Claim Term | ISM – 102(b) (incorp. by ref.) / 103 (printed publication) | |
|---------------------|--|---|--|
| ‘203 | | <p>“In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment.” (174) [SYM_P_0077182]</p> <p>“The DIDS components include the DIDS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network.” (168) [SYM_P_0077176]</p> <p>“In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS’s (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS’s would report the occurrence of an incident involving user “guest” on the target machine, DIDS would also report that user “guest” was really, for example, user “smith” on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the “chain” to find the initial launching point of the attack.” (168) [SYM_P_0077176]</p> | |
| 9 | The method of claim 1, wherein deploying the network monitors includes | <p>See ‘203 claim 8</p> <p>“The ISM model links together security systems monitoring</p> | <p>See ‘203 claim 8</p> <p>“The ISM model links together security systems monitoring</p> |

**Internetwork Security Monitor
“ISM”**

| Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|--------------|---|---|---|
| ‘203 | deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network. | <p>particular domains (e.g., a DIDS-monitored domain) via standard information exchange protocols such as the Common Management Information Protocol (CMIP) to create a large-scale, highly distributed intrusion detection system.” (268)</p> <p>[SYM_P_0069250]</p> | <p>particular domains (e.g., a DIDS-monitored domain) via standard information exchange protocols such as the Common Management Information Protocol (CMIP) to create a large-scale, highly distributed intrusion detection system.” (268)</p> <p>[SYM_P_0069250]</p> |

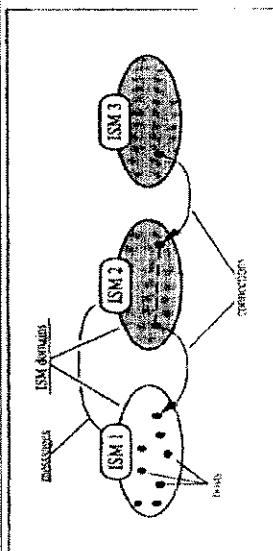
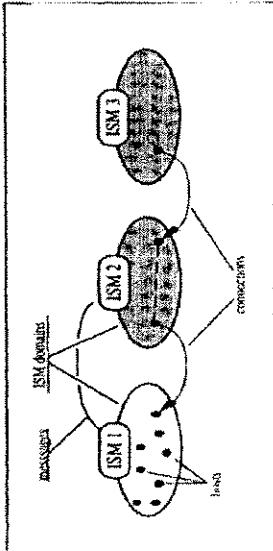
“The ISM model also allows ISMs to be grouped hierarchically. For example, ‘ISM1’ may monitor a domain which is divided into three sub-domains, each with its own ISM sub-monitors. This hierarchical structure provides two major benefits. First, because the ‘ISM1’ domain can look into its sub-domains, it can aggregate a user’s activities across these sub-domains.” (269)

[SYM_P_0069251]

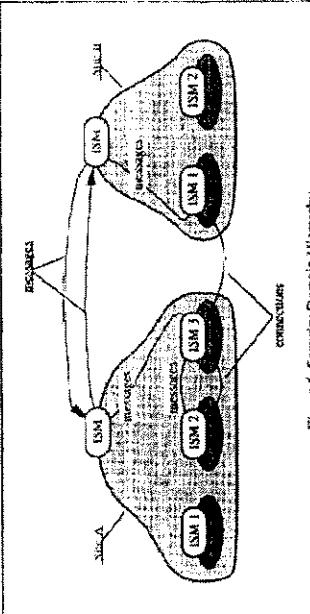
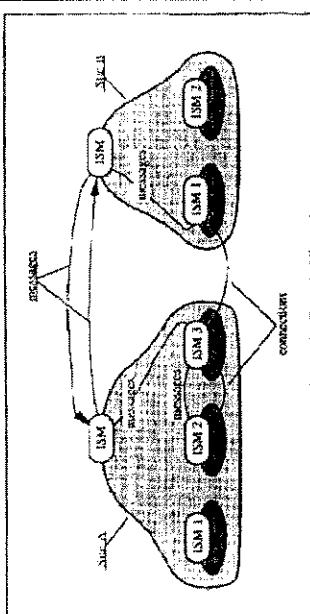
“An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines.” (270)

[SYM_P_0069252]

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|--|--|---|
| | |  <p>Figure 5. ISM Security Domains (269) [SYM_P_0069251]</p> |  <p>Figure 5. ISM Security Domains (269) [SYM_P_0069251]</p> <p>See '203 claim 8 and claim 9</p> <p>“Site A is composed of three ISM sub-domains, and site B is composed of two sub-domains. When a host in site A's third domain connects to a host in site B's first domain, site B's first domain cannot “see” site A's domain hierarchy, so it must send all queries to site A's parent ISM. Likewise, if site A's third domain queries site B for an analysis of the connection, the domain must send the query to site B's parent ISM. Importantly, to protect site A's internal structure, site A's third domain monitor performs its query through site A's parent ISM. Otherwise, a user at site B could determine site A's internal structure by “probing” site A and observing which internal ISMs respond to which probes.</p> |
| 10 | The method of claim 9, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network. | | |

**Internetes Security Monitor
“ISM”**

| | | | |
|------------------------------------|--|--|---|
| ‘203 Claim number | Claim Term ISM – 102(b) (printed publication) | <p>Meanwhile, site A's internal ISM domain monitors may continue to query each other locally (see Figure 6).” (270) [SYM_P_0069252]</p>  <p>Figure 6. Security Domain Hierarchy</p> | <p>ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)</p> <p>Meanwhile, site A's internal ISM domain monitors may continue to query each other locally (see Figure 6).” (270) [SYM_P_0069252]</p>  <p>Figure 6. Security Domain Hierarchy</p> |
|------------------------------------|--|--|---|

**Internetwor Security Monitor
“ISM”**

| ‘203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|---|---|
| 11 | The method of claim 9, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another. | <p>In extending the LAN monitoring capabilities into an internetwork environment, we are exploring the feasibility of different design alternatives for distributed-network traffic monitoring and analysis, including the following hierarchical architecture. Under this architecture, independent monitors are placed at various locations over an internetworked environment. These monitors exchange and share information (including those on hypothesized attacks) to detect possible security breaches. Subnetworks, in turn, exchange information among one another to detect inter-subnetwork attacks. (263) [SYM_P_0069245]</p> <p>“Multiple DIDS-like monitors, called ISM domain monitors, communicating through well-defined protocols form the core of the distributed ISM.” (264) [SYM_P_0069246]</p> | <p>between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly reports from the monitors.” (169) [SYM_P_0077177]</p> <p>In extending the LAN monitoring capabilities into an internetwork environment, we are exploring the feasibility of different design alternatives for distributed-network traffic monitoring and analysis, including the following hierarchical architecture. Under this architecture, independent monitors are placed at various locations over an internetworked environment. These monitors exchange and share information (including those on hypothesized attacks) to detect possible security breaches. Subnetworks, in turn, exchange information among one another to detect inter-subnetwork attacks. (263) [SYM_P_0069245]</p> <p>“Multiple DIDS-like monitors, called ISM domain monitors, communicating through well-defined protocols form the core of the distributed ISM.” (264) [SYM_P_0069246]</p> <p>“5.1 ISM PEER-LEVEL COMMUNICATION</p> <p>An ISM is responsible for a specific set of hosts. When a user initiates a connection from a host in one ISM domain to a host in a second ISM domain, the ISMs may exchange information to allow a more accurate analysis of the security state of their own domains. At a minimum, an ISM must be able to identify the</p> |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|------------|---|
| | | <p>Source (local or external to the domain) for connections leaving its domain. If the user initiating the connection originated inside the ISM domain, the ISM need only respond that the connection began internally and not reveal the actual origin of the user. If the connection originated outside the ISM domain (e.g., the user merely passed through the domain), the ISM must respond with the host-to-host connection definition of the connection entering the domain. This minimum capability of an ISM prevents an intruder from exploiting the domain in an attempt to disguise his origin. The protocol to support this functionality is presented below:</p> <ul style="list-style-type: none"> • GET TIME <time> • GET CONNECTION TCP/TP-DEF <def> TIME <time> • GET ORIGIN CONN-ID <id> <p>The first request allows an ISM to synchronize its clock to the remote ISM. An alternate, and preferred method is to assume all monitors are running under a time protocol (e.g., the network time protocol, NTP). The second request (with the time given in the remote ISM's time frame) returns an identifier, which can be used to make further requests. The third request, fulfilling the minimum requirement for an ISM, returns the origin of the user (relative to the local ISM) as either local to the domain or external (including the TCP/IP-DEF).</p> <p>source (local or external to the domain) for connections leaving its domain. If the user initiating the connection originated inside the ISM domain, the ISM need only respond that the connection began internally and not reveal the actual origin of the user. If the connection originated outside the ISM domain (e.g., the user merely passed through the domain), the ISM must respond with the host-to-host connection definition of the connection entering the domain. This minimum capability of an ISM prevents an intruder from exploiting the domain in an attempt to disguise his origin. The protocol to support this functionality is presented below:</p> <ul style="list-style-type: none"> • GET TIME <time> • GET CONNECTION TCP/TP-DEF <def> TIME <time> • GET ORIGIN CONN-ID <id> <p>The first request allows an ISM to synchronize its clock to the remote ISM. An alternate, and preferred method is to assume all monitors are running under a time protocol (e.g., the network time protocol, NTP). The second request (with the time given in the remote ISM's time frame) returns an identifier, which can be used to make further requests. The third request, fulfilling the minimum requirement for an ISM, returns the origin of the user (relative to the local ISM) as either local to the domain or external (including the TCP/IP-DEF).</p> |

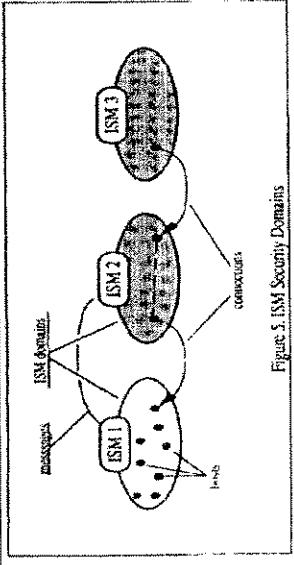
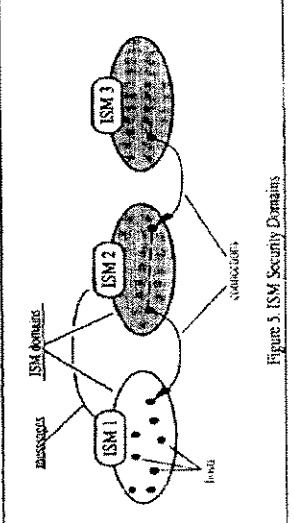
**Internetes Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) Other functionality for an ISM, while helpful but not required, includes the ability to analyze the activity within the domain for intrusive activity. Access to this analysis by external ISMs are made by the following requests: <ul style="list-style-type: none"> • GET ANALYSIS CONN-ID <id> • GET ANALYSIS HOST-ID <host-address> • GET ANALYSIS SERVICE <service-name> • GET ANALYSIS VULNERABILITY <vulnerability-id> The first request returns a value between 0 and 100, which indicates whether or not the ISM believes that the user owning the connection given by <id> is behaving intrusively. The second request also returns a value between 0 and 100, indicating whether or not the ISM believes that the host is associated with intrusive activity. The host does not necessarily have to be within the ISM's domain. For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile user on it. The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet worm exploited a hole in the mail service). The last request returns a value between 0 and 100 indicating the ISM's belief that a particular vulnerability has recently been exploited. To perform this, the ISM must have a |
|-------------------------|------------|--|
| | | |

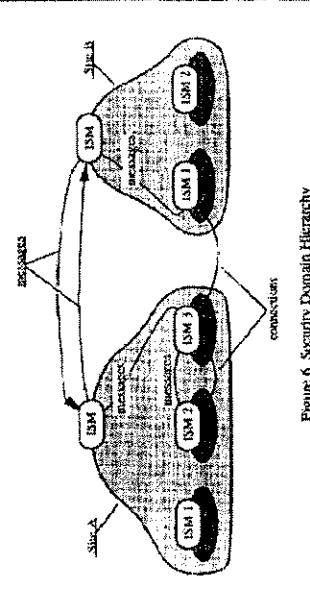
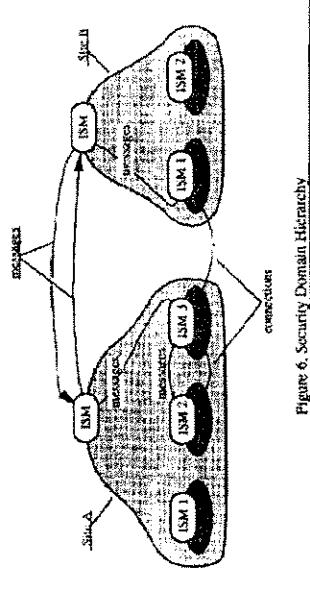
**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|------------|---|
| | | <p>catalog of known vulnerabilities and signatures to detect their [attempted] exploitation. Due to the sensitive nature of vulnerabilities, some ISMs (e.g., those at government sites) may have a more complete listing than other ISMs (e.g., those at universities).</p> <p>As an example, Figure 5 shows three ISM domains in which a single user accesses hosts in all three domains. ISM1 is able to observe all hosts within its domain; however, the hosts inside the second and third domains are hidden from ISM1's view. When a user connects to ISM1's domain, ISM1 queries ISM2 for the source of the connection, and ISM2 responds that the source is external and supplies the TCP/IP definition of the connection to ISM1. ISM1 can use this definition to query ISM3 and determine whether the source of the connection into ISM1 is somewhere inside of ISM3.”</p> <p>catalog of known vulnerabilities and signatures to detect their [attempted] exploitation. Due to the sensitive nature of vulnerabilities, some ISMs (e.g., those at government sites) may have a more complete listing than other ISMs (e.g., those at universities).</p> <p>As an example, Figure 5 shows three ISM domains in which a single user accesses hosts in all three domains. ISM1 is able to observe all hosts within its domain; however, the hosts inside the second and third domains are hidden from ISM1's view. When a user connects to ISM1's domain, ISM1 queries ISM2 for the source of the connection, and ISM2 responds that the source is external and supplies the TCP/IP definition of the connection to ISM1. ISM1 can use this definition to query ISM3 and determine whether the source of the connection into ISM1 is somewhere inside of ISM3.”</p> |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|--|
| | | <p>“Site A is composed of three ISM sub-domains, and site B is composed of two sub-domains. When a host in site A’s third domain connects to a host in site B’s first domain, site B’s first domain cannot “see” site A’s domain hierarchy, so it must send all queries to site A’s parent ISM. Likewise, if site A’s third domain queries site B for an analysis of the connection, the domain must send the query to site B’s parent ISM. Importantly, to protect site A’s internal structure, site A’s third domain monitor performs its query through site A’s parent ISM. Otherwise, a user at site B could determine site A’s internal structure by “probing” site A and observing which internal ISMs respond to which probes. Meanwhile, site A’s internal ISM domain monitors may continue to query each other locally (see Figure 6).” (270)</p> <p>(268-269) [SYM_P_0069250- SYM_P_0069251]</p>  <p>Figure 5: ISM Security Domains</p> <p>“Site A is composed of three ISM sub-domains, and site B is composed of two sub-domains. When a host in site A’s third domain connects to a host in site B’s first domain, site B’s first domain cannot “see” site A’s domain hierarchy, so it must send all queries to site A’s parent ISM. Likewise, if site A’s third domain queries site B for an analysis of the connection, the domain must send the query to site B’s parent ISM. Importantly, to protect site A’s internal structure, site A’s third domain monitor performs its query through site A’s parent ISM. Otherwise, a user at site B could determine site A’s internal structure by “probing” site A and observing which internal ISMs respond to which probes. Meanwhile, site A’s internal ISM domain monitors may continue to query each other locally (see Figure 6).” (270)</p> <p>(268-269) [SYM_P_0069250- SYM_P_0069251]</p>  <p>Figure 5: ISM Security Domains</p> |

**Internet Security Monitor
“ISM”**

| | | | |
|--|--|---|--|
| ‘203 Claim number | Claim Term [SYM_P_0069252] | ISM – 102(b) (printed publication) [SYM_P_0069252] | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) [SYM_P_0069252] |
| | |  <p>Figure 6. Security Domain Hierarchy</p> |  <p>Figure 6. Security Domain Hierarchy</p> |
| 12 An enterprise network monitoring system comprising: a plurality of network monitors deployed within an enterprise network; said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data selected from the following categories: | See ‘203 claim 1 See ‘203 claim 1 | See ‘203 claim 1 See ‘203 claim 1 | See ‘203 claim 1 See ‘203 claim 1 |

330289_1

78

**Internetes Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|---|--|
| | {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}. | | |
| 13 | said network monitors generating reports of said suspicious activity; and one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity. | See '203 claim 1 See '203 claim 1 | See '203 claim 1 See '203 claim 1 |
| 14 | The system of claim 12, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities. | See '203 claim 2 See '203 claim 2 | See '203 claim 3 See '203 claim 3 |

**Internetes Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|---|--|
| 15 | countermeasures to a suspected attack. | See '203 claim 4 | See '203 claim 4 |
| 16 | The system of claim 12, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools. | | |
| 17 | The system of claim 12, wherein the enterprise network is a TCP/IP network. | See '203 claim 5 | See '203 claim 5 |
| 18 | The system of claim 12, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}. | See '203 claim 8 | See '203 claim 8 |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term the enterprise network. | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|--|---------------------------------------|--|
| 19 | The system of claim 18, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity. | See '203 claim 8 | See '203 claim 8 |
| 20 | The system of claim 12, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network. | See '203 claim 9 | See '203 claim 9 |
| 21 | The system of claim 20, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity. | See '203 claim 10 | See '203 claim 10 |

**Internetwork Security Monitor
“ISM”**

| '203 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|----------------------------------|---|---|--|
| 22 | The system of claim 20, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another. | See '203 claim 11 | See '203 claim 11 |

**Internetes Security Monitor
“ISM”**

| '212 Claim number | Claim Term | ISM – 102(b) (printed publication) | ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication) |
|-------------------------|---|--|--|
| 1 | Method for monitoring an enterprise network, said method comprising the steps of: deploying a plurality of network monitors in the enterprise network; detecting, by the network monitors, suspicious network activity based on analysis of network traffic data, wherein at least one of the network monitors utilizes a statistical detection method; | See '203 claim 1 See '203 claim 1 See '203 claim 1 See '203 claim 1 See '203 claim 1 | <p>See '203 claim 1</p> <p>Access to this analysis by external ISMs are made by the following requests:</p> <ul style="list-style-type: none"> • GET ANALYSIS CONN-ID <id> • GET ANALYSIS HOST-ID <host-address> • GET ANALYSIS SERVICE <service-name> • GET ANALYSIS VULNERABILITY <vulnerability-id> <p>... The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet worm exploited a hole in the mail service).” (268-269)</p> <p>... The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet worm exploited a hole in the mail service).” (268-269)</p> |